UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,293	09/16/2005	Munetake Ebihara	277771US6PCT	5131

22850 7590 12/02/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SU, EMILE	
ART UNIT	PAPER NUMBER
4156	
NOTIFICATION DATE	DELIVERY MODE
12/02/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/549,293	**Applicant(s)** EBIHARA ET AL.	
	Examiner EMILE SU	**Art Unit** 4156	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Acknowledgements

1. This Office Action is in response to Applicant's Amendment filed October 10, 2008. The Amendment has been entered.

2. The previous objection to the Title and objections to Claims 1-4 and 8 are withdrawn; the previous 35 U.S.C. § 112, Second Paragraph rejections of Claims 1-7 are withdrawn; the previous 35 U.S.C. § 101 rejections of Claims 1-5, 7, and 8 are withdraw in light of Applicant's Amendment.

3. Claims 1-8 have been amended. Claims 9 and 10 are newly added claims.

4. **Claims 1-10** are currently pending and have been examined.

5. **Claims 1-10** are rejected.

6. This Office Action is made **FINAL**.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. **Claims 1–3, 5, 6, and 8-10** rare rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al., U.S. Patent No. 6,253,193 (hereinafter Ginter) in view of Hughes, U.S. Patent No. 6,748,537 (hereinafter Hughes).

With respect to Claim 1, Ginter teaches a computer-readable storage medium comprising:

a first (i.e. PPE A, see Ginter, Column 218, Lines 33-38) execution file (i.e. contain executable code, see Ginter, Column 86, Lines 36-48) recorded on said computer-readable storage medium (i.e. stored in CD-ROM, see Ginter, Column 62, Line 43 to Column 63, Line 17) using a copy protection mechanism (i.e. rights protection mechanism, see Ginter, Column 2, Line 61 through Column 3, Line 9), said first execution file including

authenticating means for performing an authentication process with a second (i.e. PPE B, see Ginter, Column 218, Lines 33-38) execution file (i.e. establishes and authenticates, see Ginter, Column 12, Lines 33-39),

key obtaining means for obtaining unique key information unique to said first execution file (i.e. unique session key, see Ginter, Column 219, Line 52 through Column 220, Line 19), and

transmitting means for transmitting said unique key information to said second execution file (i.e. Deliver protected session key, see Ginter, Column 219, Line 52 through Column 220, Line 19),

an information processing apparatus including a processor (i.e. contains a processor to perform instructions, see Ginter, Column 59, Line 60 through Column 60, Line 8), said second execution file generates (i.e. decrypt secure information, see Ginter, Column 71, Lines 32-41; also see Column 200-201 for secure communication using keys) a content key (i.e. content … that may be encrypted using one or more content key, see Ginter, Column 130, Lines 25-40) from said unique key information (i.e. decryption keys, see Ginter, Column 66, Lines 12-18; note that unique key information is a session key now being used for decrypting), decrypts encrypted content using the content key (i.e. decrypt the object's content, see Ginter, Column 206, Line 61 through Column 207, Line 7), and reproduces the decrypted content (i.e. playing said music, see Ginter, Column 320, Line 62 through Column 321, Line 18).

However, Ginter does not specifically teach wherein a file is executed when inserted into an information processing apparatus.

Hughes does disclose wherein a file is executed when inserted into an information processing apparatus (i.e. player software on the CD is automatically executed, see Hughes, Column 3, Line 32 through Column 4, Line 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to automate execution of a file upon insertion, because it is convenient for users unfamiliar with electronic equipment and gives the content owner control over how content should be managed.

As to Claim 2, see discussion of Claim 1 above. Ginter further teaches wherein said unique key information is used to encrypt encryption key information for encrypting a content (i.e. Master Key, see Ginter, Column 212, Lines 12-38; note master key is a concept of communicating other keys in a secure way).

As to Claim 3, see discussion of Claim 2 above. Ginter further teaches wherein at least one of said second execution file (i.e. code that is executed, see Ginter, Column 62, Line 58 through Column 63, Line 17) and said content is recorded on said computer-readable storage medium (i.e. encrypting information before storing it, see Ginter, Column 62, Line 42 through Column 63, Line 17).

With respect to Claim 5, Ginter teaches an information processing apparatus (i.e. circuit, see Ginter, Column 59, Line 60 through Column 60, Line 8) into which a computer-readable storage medium is inserted (i.e. stored in CD-ROM, see Ginter, Column 62, Line 43 to Column 63, Line 17), said computer-readable storage medium including a first (i.e. PPE A, see Ginter, Column 218, Lines 33-38) execution file (i.e. contain executable code, see Ginter, Column 86, Lines 36-48) recorded using a copy protection mechanism (i.e. rights protection mechanism, see Ginter, Column 2, Line 61 through Column 3, Line 9), said information processing apparatus comprising:

a processor (i.e. contains a processor to perform instructions, see Ginter, Column 59, Line 60 through Column 60, Line 8); and

a second (i.e. PPE B, see Ginter, Column 218, Lines 33-38) execution file for reproducing (i.e. playing said music, see Ginter, Column 320, Line 62 through Column 321, Line 18) and encrypted content (i.e. decrypt the object's content, see Ginter, Column 206, Line 61 through Column 207, Line 7; note that the content is encrypted for decryption),

wherein said second execution file includes authenticating means for performing an authentication process with said first execution file (i.e. three-way X.509 public key protocol steps, see Ginter, Column 218, Line 60 through Column 220, Line 19), key generating means for generating (i.e. decrypt secure information, see Ginter, Column 71, Lines 32-41; also see Column 200-201 for secure communication using keys) encryption key information (i.e. content … that may be encrypted using one or more content key, see Ginter, Column 130, Lines 25-40) based on unique key information obtained from said first execution file (i.e. decryption keys, see Ginter, Column 66, Lines 12-18; note that unique key information is a session key now being used for decrypting), decrypting means for decrypting said encrypted content using said encryption key information (i.e. decrypt the object's content, see Ginter, Column 206, Line 61 through Column 207, Line 7), and reproducing means for reproducing the decrypted content (i.e. playing said music, see Ginter, Column 320, Line 62 through Column 321, Line 18).

However, Ginter does not specifically teach wherein file is executed when said computer-readable storage medium is inserted into the information processing apparatus.

Hughes does disclose wherein file is executed when said computer-readable storage medium is inserted into the information processing apparatus (i.e. player software on the CD is automatically executed, see Hughes, Column 3, Line 32 through Column 4, Line 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to automate execution of a file upon insertion, because it is convenient for users unfamiliar with electronic equipment and gives the content owner control over how content should be managed.

As to Claim 6, see discussion of Claim 5 above. Ginter further teaches wherein said encrypted content is recorded on one of said computer-readable storage medium (i.e. encrypting information before storing it, see Ginter, Column 62, Line 42 through Column 63, Line 17; note secondary storage is computer-readable storage medium), in said information processing apparatus, and in a different information processing apparatus (i.e. semiconductor memory, see Ginter, Column 21, Lines 5-42).

With respect to Claim 8, Ginter teaches an information processing method of an information processing apparatus (i.e. contains a processor to perform instructions, see Ginter, Column 59, Line 60 through Column 60, Line 8), a computer-readable storage medium (i.e. stored in CD-ROM, see Ginter, Column 62, Line 43 to Column 63, Line 17) having a first (i.e. PPE A, see Ginter, Column 218, Lines 33-38) execution file (i.e. contain executable code, see Ginter, Column 86, Lines 36-48) recorded therein using a copy protection mechanism (i.e. rights protection mechanism, see Ginter, Column 2, Line 61 through Column 3, Line 9), said information processing method comprising:

performing by a processor (i.e. contains a processor to perform instructions, see Ginter, Column 59, Line 60 through Column 60, Line 8), authentication process with said first execution file (i.e. three-way X.509 public key protocol steps, see Ginter, Column 218, Line 60 through Column 220, Line 19); generating (i.e. decrypt secure information, see Ginter, Column 71, Lines 32-41; also see Column 200-201 for secure communication using keys) encryption key information (i.e. content … that may be encrypted using one or more content key, see Ginter, Column 130, Lines 25-40) based on unique key information obtained from said first execution file (i.e. decryption keys, see Ginter, Column 66, Lines 12-18; note that unique key information is a session key now being used for decrypting);

decrypting an encrypted content using said encryption key information (i.e. decrypt the object's content, see Ginter, Column 206, Line 61 through Column 207, Line 7); and reproducing the decrypted content (i.e. playing said music, see Ginter, Column 320, Line 62 through Column 321, Line 18).

However, Ginter does not specifically teach into which a computer-readable storage medium is inserted.

Hughes does disclose into which a computer-readable storage medium is inserted (i.e. when the storage medium is inserted, see Hughes, Column 3, Line 32 through Column 4, Line 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create an computer-readable storage medium that can be inserted, because it is a removable medium is convenient to transport across different equipment (see Hughes, Column 2, Lines 7-50).

As to Claim 9, see discussion of Claim 2 above. Ginter further teaches wherein at least one of said second execution file (i.e. execute VDE related instructions, see Ginter, Column 21, Lines 5-42) and said content is recorded in said information processing apparatus (i.e. semiconductor memory, see Ginter, Column 21, Lines 5-42).

As to Claim 10, see discussion of Claim 2 above. Ginter teaches the invention substantially as claimed. However, Ginter does not specifically teach wherein at least one of said second execution file and said content is recorded in a different information processing apparatus.

Hughes does disclose wherein at least one of said second execution file and said content is recorded in a different information processing apparatus (i.e. transferred to another computer, see Hughes, Column 2, Lines 22-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to store content in a second (i.e. PPE B, see Ginter, Column 218, Lines 33-38) apparatus, because this reduces the memory load necessary for the first apparatus.

9. **Claims 4 and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter in view of Hughes as applied to Claims 1-3 above, and further in view of Matsuyama et al., U.S. Patent Application Publication 2002/0026581 (hereinafter Matsuyama).

With respect to Claim 4, Ginter and Hughes disclose the invention substantially as claimed. However, Ginter and Hughes do not specifically disclose encrypting digital signature information attached to said content; and said transmitting means transmits said content to said second execution file based on said digital signature information.

Matsuyama does teach encrypting digital signature information attached to said content (i.e. attach his/her signature encrypted with the private key to a document, see Matsuyama, ¶169); and said transmitting means transmits said content to said second execution file based on said digital signature information (i.e. transmitted by means of encryption using the public key certificate, see Matsuyama, ¶165; also see ¶160-169).

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt digital signature information and transmit data as taught by Matsuyama, because digital signature can verify the authenticity of the sender (see Matsuyama, ¶166).

With respect to Claim 7, Ginter and Hughes disclose the invention substantially as claimed. Ginter further teaches said unique key information is used to encrypt encryption key information (i.e. Master Key, see Ginter, Column 212, Lines 12-38; note master key is a concept of communicating other keys in a secure way). However, Ginter and Hughes do not specifically disclose encrypting digital signature information attached to said encrypted content, and receiving means for receiving said encrypted content based on said digital signature.

Matsuyama does teach encrypting digital signature information attached to said encrypted content (i.e. attach his/her signature encrypted with the private key to a document, see Matsuyama, ¶169), and receiving means for receiving said encrypted content (i.e. Upon reception of the document, see ¶169) based on said digital signature (i.e. transmitted by means of encryption using the public key certificate, see Matsuyama, ¶165; also see ¶160-169).

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypted digital signature information and transmit data as taught by Matsuyama, because digital signature can verify the authenticity of the sender (see Matsuyama, ¶166).

Response to Arguments

10. Applicant's amendments have overcome the Objections, Rejections under 35 U.S.C. § 112, Second Paragraph, and Rejections under 35 U.S.C. § 101 from the previous Office Action.

The previous objection to the Title and objections to Claims 1-4 and 8 are withdrawn in light of Applicant's amendments to the Title and Claims 1 and 8.

The previous 35 U.S.C. § 112 Second Paragraph rejections of Claims 1-7 are withdrawn in light of Applicant's amendments to Claims 1-7.

The previous 35 U.S.C. § 101 rejections of Claims 1-5, 7, and 8 are withdraw in light of Applicant's amendments to Claims 1, 5, and 8.

11. Applicant's arguments filed October 10, 2008 with respect to **Claims 1-8** have been considered but are moot in view of the new ground(s) of rejection. Applicant's amendment necessitated the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EMILE SU whose telephone number is (571)270-7040. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, CHARLES R. KYLE can be reached on (571) 272-6746. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/EMILE SU/
Examiner, Art Unit 4156
November 13, 2008

/Charles R. Kyle/
Supervisory Patent Examiner, Art Unit 4156